



(19)

Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 0 752 143 B1

(12)

## EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention  
of the grant of the patent:  
**29.12.1997 Bulletin 1997/52**

(51) Int Cl.: **G07C 9/00, A61B 5/117**(21) Application number: **95914734.9**(86) International application number:  
**PCT/US95/03295**(22) Date of filing: **15.03.1995**(87) International publication number:  
**WO 95/26013 (28.09.1995 Gazette 1995/41)**

## (54) BIOMETRIC, PERSONAL AUTHENTICATION SYSTEM

BIOMETRISCHES PERSONENAUTHENTISATIONSSYSTEM

SYSTEME D'IDENTIFICATION BIOMETRIQUE DE PERSONNES

(84) Designated Contracting States:  
**DE ES FR GB IT NL**

- BLAN, Bradford L.  
Birmingham, AL 35223 (US)
- ARNESEN, Michael R.  
Westminster, MD 21157 (US)

(30) Priority: **24.03.1994 US 217433**

(74) Representative: **VOSSIUS & PARTNER**  
**Siebertstrasse 4**  
**81675 München (DE)**

(43) Date of publication of application:  
**08.01.1997 Bulletin 1997/02**

(56) References cited:

- |                        |                        |
|------------------------|------------------------|
| <b>EP-A- 0 082 304</b> | <b>EP-A- 0 121 222</b> |
| <b>WO-A-90/08366</b>   | <b>DE-A- 3 834 048</b> |
| <b>DE-C- 3 731 773</b> | <b>NL-A- 8 503 290</b> |
| <b>US-A- 4 869 254</b> | <b>US-A- 5 078 136</b> |
| <b>US-A- 5 103 486</b> |                        |

(73) Proprietor: **MINNESOTA MINING AND  
MANUFACTURING COMPANY**  
St. Paul, Minnesota 55133-3427 (US)

(72) Inventors:

- OSTEN, David W.  
Saint Paul, MN 55133-3427 (US)
- CARIM, Hatim M.  
Saint Paul, MN 55133-3427 (US)

EP 0 752 143 B1

Note: Within nine months from the publication of the mention of the grant of the European patent, any person may give notice to the European Patent Office of opposition to the European patent granted. Notice of opposition shall be filed in a written reasoned statement. It shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

**Description**

**Government Rights**

5 This invention was made with U.S. Government support under Local Subcontract SO-124465-S and MDA904-93-C4074. The U.S. Government has certain rights in this invention.

**Field of the Invention**

10 This invention relates to biometric, personal authentication systems that authenticate identities of individuals.

**Background of the Invention**

15 Personal recognition systems generally utilize a single highly specific characteristic for identifying valid access requests, sometimes in association with another method of individual authentication.

Published patent application NL 8503290, (Sibum) according to an uncertified English translation teaches identifying a person by recognition of a stored pattern, e.g. fingerprint, preventing unauthorized access or use, using pattern analysis with determination of body heat and/or hair size and color to prevent use of a falsified replica of the fingerprint.

20 Thus, this document teaches identifying a person by recognition of at least an inherently specific biometric parameter of said person, e.g. finger print, and detecting a non-specific biometric parameter comparable to physiological norms such as the body heat during the authentication.

Published PCT patent application WO 90/08366 (Clayden) teaches identification of a person by monitoring one or a number of "biometric" parameters such as bone structure, temperature, fingernail pattern, creases in the palm or fingers of the hand and comparing the monitored data with stored characteristics. Further, teachings include reference to speech, handwriting and piano keyboard "signatures".

25 U.S. Pat. No. 4,896,363, (Taylor) teaches a method for analysis and comparison of a "live" fingerprint to a stored record and an apparatus for functional use of the method. Commercial products described in Taylor include personal access apparatus manufactured by Thumbscan Corporation.

30 U.S. Pats. Nos. 4,869,254 and 5,078,136 (both Stone et al.) teach a method for non-invasive measurement and calculation of oxygen saturation on blood in the human body under transient conditions and describe apparatus for functional use of the method. Commercial products described in Stone et al. are widely identified as pulse oximeters.

35 U.S. Pat. No. 5,103,486 (Grippi) teaches a scanning of a combination of fingerprint with an overwritten projection of a signature to identify an individual, and claims the projection of "any biological feature of the user". A biological feature is described as live skin tissue.

**Summary of the Invention**

None of the authentication, recognition, or access control systems in the art recognize the problem that biometric devices can be circumvented by presenting the biometric pattern of an authorized individual seeking biometric, personal authentication who has been incapacitated, dismembered, or is deceased at the time of attempted authentication, recognition, or access.

Stated another way, none of the authentication, recognition, or access control systems in the art recognize the possibility that biometric parameters can be correlated or otherwise interrelated in order to assure that an individual seeking biometric, personal authentication is actually present for authentication. Existing devices can be circumvented by someone, other than the genuine person seeking authentication, actually presenting the biometric pattern of an authorized individual seeking biometric, personal authentication.

For example, a fingerprint analysis that does not recognize whether the finger is attached to a living human being can be circumvented by electronic or photographic reconstructions of the fingerprint or dismemberment of the finger. Other evidence the art presently employs for confirmation can be circumvented by use of subterfuge and substitution.

50 The present invention solves a problem unrecognized in the art by providing a biometric, personal authentication system that requires correlation among a unique, inherently specific biometric parameter with at least one non-specific biometric parameter having measurable variability during the time of authentication in a physiologically acceptable range.

Previously, the art has considered two kinds of errors. The first kind is where the authentication system would erroneously reject authentication of a truly authorized user. The second kind of error is where the authentication system would erroneously accept authentication of a truly unauthorized user. Both kinds of error are based on the accuracy and precision of authentication based on a unique, inherently specific biometric parameter. The parameter can be too severely applied, (rejecting authentication when it should be accepted,) or too loosely applied, (accepting authentication

EP 0 752 143 B1

when it should be rejected). In general, the two kinds of errors for a recognition system using a single, unique, inherently specific biometric parameter are inversely related. Reducing the error rate for false rejection increases the false acceptance rate, and vice versa. Authentication systems, especially access systems, are faced with this dilemma.

The present invention considers a third kind of error and solves a problem that the art has not recognized. An unrecognized third possible error is where the authentication system would erroneously accept authentication of a truly unauthorized user attempting to gain access using the pattern of a unique, inherently specific biometric parameter from an authorized user. The errors of the first and second kind, and solutions to treat such errors, do not consider or adequately measure the risk of circumvention of the authentication system.

The present invention solves errors of the third kind by providing an authentication system that recognizes a unique, inherently specific biometric parameter and other non-specific biometric parameters that need not be unique to the individual but are comparable to physiological norms and are variable during the time of authentication.

The present invention solves the problem that at least two modes of biometric recognition must fail or be circumvented in order to authenticate an unauthorized user.

"Biometric parameters" means dimensional and physiological characteristics of an individual human. Some biometric parameters (e.g., fingerprints (including thumbprints), palm prints, pore prints, voice prints, handwriting (including signature), and retinal configurations), are both unique and inherently specific and are relatively easy to copy and reproduce or model for later comparison for purposes of authentication. Fingerprint analysis refers to the identification and measurement of minutia points (bifurcations and end points). Pore print analysis refers to the identification and measurement of pores within the ridges of the fingers.

Other biometric parameters are non-specific and not unique to an individual. Some non-specific biometric parameters include dimensional characteristics (e.g., bone structure, and physical dimensions) and skin temperature that are not likely to have some variability during the time required for authentication and physiological characteristics (e.g., electrocardiographic (EKG) signals, pulse, and spectral characteristics of human tissue) that are likely to have some measurable variability during the time required for authentication. Of the two, physiological characteristics are more meaningful to biometric, personal authentication because such physiological characteristics are more difficult to simulate because such measurements are observable within physiological ranges, variable in time and, in characteristics such as EKG and pulse, synchronizable within a single human body.

One or more non-specific biometric parameters used in combination with one or more unique, inherently specific biometric parameters provides extremely high precision protection against circumvention, and does not require time consuming and inordinate measurement for authentication for purposes such as access control to a secure function or fitness to perform a function. Further non-specific physiological characteristics such as blood alcohol content or levels of controlled chemical substances (e.g., legal drugs used in illegal quantities or at illegal times or illegal drugs) in the body could be used to determine if an otherwise authorized user is authenticated to be in acceptable physical condition to be granted access to a motor vehicle or other facility or equipment.

The biometric, personal authentication system of the present invention comprises:

- (a) storage subsystem to store a unique, inherently specific biometric parameter from at least one individual in a species;
- (b) first recognition subsystem to detect the unique, inherently specific biometric parameter in an individual seeking personal authentication;
- (c) second recognition subsystem to detect at least one non-specific biometric parameter of a physiological characteristic having measurable variability during the time of authentication in the individual seeking personal authentication;
- (d) first comparison subsystem to compare the unique, inherently specific biometric parameter detected by the first recognition subsystem with the unique, inherently specific biometric parameter stored in the storage subsystem;
- (e) second comparison subsystem to compare each non-specific biometric parameter to physiological norms for the species within an acceptable range; and
- (f) authentication subsystem to confirm identity of the individual seeking personal authentication by evaluating the comparisons made by first comparison subsystem and second comparison subsystem.

Desirably, an optional step (g) includes a subsystem to use successful authentication to provide access.

Preferably, the second recognition subsystem detects at least two non-specific biometric parameters with physiological correlation of the non-specific biometric parameters within an acceptable range. More preferably, the detection of at least two non-specific biometric parameters are synchronized. Examples of non-specific biometric parameters of physiological characteristics include bloodflow, spectral identity of tissue, electrocardiographic signals, pulse, blood oxygenation, hematocrit, biochemical assays of tissue, electrical plethysmography, skin exudates, mechanical properties of skin, electrical properties of skin, transpiration of gases, blood pressure, and differential blood volume.

Most preferably, the biometric, personal authentication system of the present invention utilizes fingerprint analysis (used in this invention to include thumbprint analysis) of an individual in combination with pulse oximetry and electrocardiography of the individual. The fingerprint analysis supplies the unique, inherently specific biometric parameter while the data from a pulse oximeter and EKG supplies the non-specific parameter(s), preferably both synchronized in time between two non-specific parameters and correlated between the non-specific parameters and the unique, inherently specific biometric parameter. Specifically the EKG signal as measured in real time is synchronized with the pulse measured by the pulse oximeter as change of rate of blood flow in real time.

For example, if the fingerprint analysis matches the unique, inherently specific biometric parameter, and if the pulse oximeter data of pulse and percentage oxygen saturation and EKG as non-specific biometric parameters correlate within acceptable norms, and if pulse is determined by two different and synchronizable methods (electrical and optical) to be synchronized, then the individual identified with the fingerprint is not incapacitated, dismembered, or deceased, and then authentication of the individual is achieved. Optionally, skin temperature can be added to provide further confirmation of viability of the individual seeking authentication.

With authentication of an individual according to the present invention, a variety of actions can be taken. Nonlimited examples of actions available to the authenticated individual include access to equipment, access to physical facilities, recognition of the individual for a variety of reasons, confirmation of presence of the individual in an authorized location or using authorized equipment, and other situations where the status of an individual is remotely determined or controlled.

Beyond the first level of authentication of an individual and authorization of entry to a physical facility or use of equipment, suitability of performance may be verified for a second level of access control through measurement of blood gases or other characteristics, such as blood alcohol or controlled chemical substances levels, that would impair the individual's operation of equipment such as a mass transit vehicle.

A feature of the present invention is that inherently specific and non-specific biometric parameters can be concurrently and non-invasively gathered for recognition, comparison, and determination of authentication.

Another feature of the present invention is that non-specific biometric parameters need not be identified to the individual seeking personal identification.

An advantage of the present invention is that individuals seeking personal authentication undergo multiple biometric parameter comparison with security measures that potentially avoid false authentication.

One optional feature of the invention includes the use of information input and data entry apparatus to minimize searching of stored data of the unique, inherently specific biometric parameter, such as by use of a personal identification number or code, a photo, or other means.

Another optional feature of the invention includes apparatus for reading and analyzing encoded and encrypted information resident on magnetic or optical media or a hologram stored on a plastic card possessed by the individual seeking authentication, rather than stored in the apparatus for receiving data of the unique, inherently specific biometric parameter.

Another optional feature of the invention is to provide additional authentication using apparatus that identifies and compares more than one unique, inherently specific biometric parameters such as written signature, retinal configuration, voice recognition, or physical dimensions of the individual or features of the individual.

#### 40 Brief Description of the Drawings

FIG. 1 is a schematic illustration of a preferred embodiment of the invention.

FIGS. 2a, 2b, and 2c are plan views of a preferred embodiment of the invention.

FIGS. 3a, 3b, and 3c are cutaway views of a preferred embodiment of the invention showing positions of the measurement apparatus.

FIG. 4 is a block diagram of the apparatus for recognizing the non-specific biometric parameter of electrocardiographic signals.

FIG. 5 is a block diagram of the apparatus for recognizing the non-specific biometric parameter of blood oxygen saturation.

FIG. 6 is a block diagram of the apparatus for recognizing the non-specific biometric parameter of skin temperature.

FIG. 7 is a flow chart for completing authentication according to the present invention.

FIG. 8 is an electrical schematic illustration of circuitry for processing the non-specific biometric parameter of electrocardiographic signals as shown in FIG. 4.

FIG. 9 is an electrical schematic illustration of circuitry for producing pulsating power to the red and IR lamps for the non-specific biometric parameter of blood oxygen saturation as shown in FIG. 5.

FIG. 10 is an electrical schematic illustration of circuitry for processing the signals indicating non-specific biometric parameter of blood oxygen saturation as shown in FIG. 5.

FIG. 11 is an electrical schematic illustration of circuitry for the temperature sensor circuit shown as a block diagram

in FIG 6.

Embodiments of the Invention

5 FIG. 1 shows a schematic of a preferred embodiment of the personal, biometric authentication system of the present invention. This embodiment is a counter top mounted access control unit containing the data entry and sensor apparatus. The access control is interconnected with a protected electronic computer system to provide authentication of the individual requesting entry and use of the system.

10 This embodiment utilizes a portion of the general purpose computer 2 for processing 6 of the non-specific biometric indicator data and processing 4 of the unique fingerprint image.

An individual seeking access first enters an identification code followed by placing both hands on contoured surfaces containing various sensors for a period of approximately ten seconds until authentication is completed successfully or unsuccessfully, and, preferably, access is granted or denied. Identification code entry 8 is a personal identification code number (PIN) or can be an identification card inserted and read to request access through the access system. Use of personal identification codes narrows the search process needed to compare the unique, inherently specific biometric parameter detected by the device with stored data. This acts to speed operations needed for establishing personal authentication. Further the PIN number can provide an additional, preliminary level of comparison in the authentication process.

20 Authentication system elements include fingerprint image sensor 10 inputing data for analysis to computer logic and memory functions 4 for unique, inherently specific identification; and non-specific biometric sensors 24, 26, and 28 with signal process functions 30 inputing information for analysis to computer system 6 to recognize electrocardiogram (EKG), pulse, and blood oxygen saturation for nonspecific biometric validation and skin temperature for further optional validation. With this combination of information the individual seeking authentication and access can be uniquely identified and a determination can be made that the individual seeking authentication is not incapacitated, dismembered, or deceased. In other words, the biological state of the individual, as measured non-invasively via physiological characteristics that vary in time during the authentication, is used with the unique, inherently specific parameter of a fingerprint to authenticate that the individual is alive and functioning with acceptable physiological conditions for authentication and resulting access.

25 Fingerprint recognition camera 10 and system 4 employs well known apparatus, circuitry, and software. The individual's fingerprint pattern is detected by camera 10 when the individual places a thumb on detector window 42, (shown on FIG. 2 and described below). The detected image is captured and analyzed by image processor 12, developed into a vector array of fingerprint minutiae which is validated by comparator 14 through correlation of the scanned image vector array with the array selected from pre-stored memory file 16 indexed by PIN. If the image matches the stored information, then output 18 of comparator 14, is turned on, signaling the decision process as diagrammed in FIG. 7 and described below.

30 Fingerprint recognition systems such as camera 10 working with system 4 are commercially available from Thumb-Scan, Inc., Lombard IL. Such system 4 is described in U.S. Pat. No. 4,896,363 (Taylor). Alternatively, camera 10 is commercially available as Model FC-11 Fingerprint Capture Station, from Digital Biometrics, of Minnetonka MN. When Digital Biometrics camera 10 is used, then frame grabber IP-8 Image Processing Board commercially available from Matrox Electronic Systems, LTD, of Dorval, Quebec, Canada is also used, along with comparison software commercially available from BlitzMatch, Inc. of Champaign, IL.

35 The pre-stored fingerprint selection pattern may be stored in a dedicated ROM memory of the fingerprint recognition system 4; or stored in the memory of computer terminal accessed by the individual through a standard key pad connected to a asynchronous I/O port; or entered into the security access system via a magnetic or optical identification card presented to the access instrument at the time of actuating the access system. The identification card may replace or supplement the entry of the PIN using the key pad.

40 Non-specific biometric recognition circuitry shown in FIG. 1 include biomedical (EKG) electrodes 24 communicating with analog signal processor 32, light emitting diode (LED) sources (one in the visible range (about 660 nm) and the other in the near infrared (NIR) range (about 910 nm)) and detector 26 communicating with timed power source and signal processor 34, for the plethysmographic signals of the blood pulse/oxygen monitor and temperature sensor 28 communicating with signal processor and ambient temperature sensor 36.

45 After analog processing, the signals are communicated to computer system 6 digitized for analysis through interface 22 (such as a RIT-815 card available from Analog Devices of Norwood, MA). The digitized signals are processed within a general purpose computer CPU, for example a IBM PS/2, available from IBM Corporation of Armonk, N.Y. The sensor processing 38 follows a logic pattern programmable by a person of ordinary skill in programming the general computer of choice. The logic pattern includes a variety of calculating, smoothing and comparing steps as shown in the flow diagram of FIG. 7. Acceptances ranges are stored in memory 20 and compared with the individual data at decision states 324, 328, 330 and 332 as further defined within the flow diagram of FIG 7.

FIG. 2 is a counter-mounted embodiment of the security access instrument, shown in three views, 2a-2c. FIG. 2a shows semi-frontal view 40-A; FIG. 2b shows side plan view 40-B; and FIG. 2c shows top plan view 40-C. Counter-mounted security access instrument 60 has a thumb or finger positioning cavity 62 preferably with an indented platten, for receiving the thumb or finger comfortably, open through front surface 64, extending to the interior of the instrument providing access to detector window 42 and other sensor elements described below, wherein the sensors are protected from stray light. The location and configuration of cavity 62 allows positioning of both left and right hand of the individual seeking authentication on biomedical electrodes 44, 46, 48, and 50 with the thumb or finger of one hand properly oriented on detector window 42 inside cavity 62. A switch (not shown) can be mounted on the instrument 60 adjacent electrodes in order to activate scanning.

Detector window 42 can be a prism for redirecting light, preferably having a coating to present a good "feel" to the user while protecting window 42.

This configuration is only one of many that would allow for positioning of the hands or other body parts in contact with the EKG electrodes while also providing positions for a selected finger or toe on the fingerprint scanner. For example, the measurement section could be essentially flat with the detector window in the center and EKG electrodes configured on either side such that a toe or finger could be positioned on the detector window and EKG contact made to parts of the hand or foot.

FIGS. 2a and 2c show a keypad 54 for entry of PIN or other coded information input and display window 56 for information and status output. This configuration can be expanded to include readers for ID cards or memory devices and sound transducers for verbal or sound tone input or output.

This counter-mounted embodiment of the security access instrument is connected by appropriate electrical cables (not shown) to a computer for power, signal and data communication. Further equipment could easily be built into the access instrument to include microprocessor and memory for handling the computer related logic functions, power supply, and output devices; such that the output of this instrument would be a simple call signal for use with a relay or other response apparatus to allow the individual access to the secured equipment or facility after authentication is obtained.

FIGS. 3a-3c show the counter-mounted embodiment of the security access instrument, in partial cutaways detailing the position of window 42 with respect to spring assembly 90 such that light emitting diodes 92 and 96 are essentially diametrically opposite photodetector 98. Alternatively, light emitting diodes 92 and 96 and photodetector 98 can be mounted above and below the thumb positioning cavity. Optional skin temperature sensor 80 is positioned next to window 42 in line with the entry axis of the thumb positioning cavity 62 to be in contact with the skin near connection of the thumbprint region of the hand.

FIGS. 4, 5, and 6 are block diagrams of circuitry for the devices for measuring the non-specific biometric parameters -- EKG, blood oxygen, pulse, and skin temperature. -- expanding the content of sensor interface electronics block 30, and sensors 24, 26 and 28.

The sensors 24 used for EKG detection are signal electrodes 102 and 104 plus ground electrode 106 shown in FIG. 4. These are the same electrodes as 46 and 48, and ground electrodes 44, and 50 (which are connected together) of FIG. 2, respectively, wherein ground electrode 106 and first biomedical electrode 104 contact the left hand and second biomedical electrode 102 contacts the right hand (not shown).

Biomedical electrodes useful in the present invention are commercially available from Minnesota Mining and Manufacturing Company, St Paul, MN. Particularly preferred are biomedical electrodes described in U.S. Pat. No. 5,012,810 (Strand et al.); U.S. Pat. Nos. 4,524,087; 4,539,996; 4,554,924; and 4,848,353 (all Engel); and U.S. Pat. No. 5,133,356 (Bryan et al.).

Electrodes 102, 104, and 106 are mounted with conductive adhesive surfaces exposed for contact with fingers or thumbs. Electrodes 102, 104, and 106 are cleaned periodically as the conductive adhesive contact surface is contaminated by dirt and dry skin flakes. Electrodes 102 and 104 are connected to the inputs of differential instrumentation amplifier 110 which provides signal amplification with high input impedance as required for efficient interface to electrodes 102 and 104. Instrumentation amplifier 110 is followed by isolation amplifier 112 to provide electrical isolation to the individual. Both instrumentation amplifier 110 and isolation amplifier 112 are powered by isolated DC-DC converter 118 providing safety protection by electrical isolation from the main power supply.

The EKG signal is processed by band pass filter 114 to eliminate unwanted noise outside the 0.05 Hz to 30 Hz frequency band and amplified by buffer amplifier 116 to compensate for signal level from the human body. The processed EKG signal output 126 is communicated to analog to digital interface 22.

A block diagram for blood oxygen saturation sensor is shown in FIG. 5. The sensor is a pulse oximeter type and is well known to those skilled in the art. The emitters and sensors of this device are located in the detector window 42 (shown in FIG. 3), delivering near infrared (NIR) and visible light at multiple wavelengths through human tissue of the thumb and detecting the transmitted light. The light emitters are powered at an alternating rate such that one light is off when the other light is on, the driving rate of the lights is at a frequency much greater than the human heart rate, for example 1500 Hz.

EP 0 752 143 B1

The detected light sampled at the same driving rate and is pulsatile in nature related directly to the normal heart pulse cycle. Change in detected light intensity at the peak and at the valley phases of a particular pulse cycle provides a relative measure of absorbance in the arterial blood. By comparing the relative absorbances at multiple wavelengths (usually about 910 nm and 660 nm), an oxygen saturation value can be determined for the blood of the subject.

5 Light source 140 delivers light at two wavelengths. One light emitting diode (LED) 142 emitting light at a wavelength of 660 nanometers and one LED 144 emitting light at a wavelength of 910 nanometers are driven by LED drive sources 148 and 150. The LEDs are timed by clock generator 146 generating intermittent on and off condition providing two distinct states for the overall light source: 910 diode on/660 diode off shown as 156, 910 diode off/660 diode on shown as 152.

10 Detector 170 transduces the transmitted light to an electrical signal with variable current silicon photodiode 172. The variable current signal is converted to a variable voltage by current to voltage amplifier 174. Detection is synchronized with the LED emitter timing, detecting and holding the light level transmitted during each of the two distinct states with sample and hold circuits 182, and 186. Each transmitted light signal includes both a DC and AC components which are separated for the blood oxygen calculation and processing in sensor processor 38. The 910 nanometer signal is amplified 190 and filtered 192 to eliminate unwanted signal above 10 Hz and communicated to interface 22 through connection 198-D. AC component is separated by 0.3 Hz high-pass filter 194, amplified by amplifier 196 and communicated to interface 22 through connection 198-A.

15 Parallel processing of the 660 nanometer signal is through channel 200, 202, 204, 206 and 208-A and 208-C.

20 The blood oxygen measurement of this system is well known and described in U.S. Pat. Nos. 4,869,254 and 5,078,136 (Stone et al.). Pulse oximeters are commercially available in the manner described by these patents, including light emitting diodes 142 and 144 and detector 170 sold by Nellcor Incorporated of Hayward, CA.

25 Processing of the pulse oximeter signal is described herein as time domain signal processing. Clearly the processing could be done in the frequency domain by digitizing the signal directly at the sensors and using digital signal processing techniques.

30 Optionally, skin temperature is measured with a solid state sensor chosen for linearity across the temperature range of the human body. Block diagram of the associated measurement circuit 250 is shown in FIGURE 6. Skin temperature sensor 252 is supplied by isolated DC/DC converter 256, for protection of the individual. Voltage from sensor 252 is linearly dependent on the temperature, is amplified and isolated from other circuitry by amplifiers 258 and 262. The temperature signal is filtered 264 to eliminate all frequencies above 0.5 Hz, to eliminate electrical noise and communicated to interface 22 through connection 272. Optionally, an ambient temperature sensor 254 may be used to compensate for environmental conditions as shown in block diagram 260. The signal from optional temperature sensor 254 is amplified by amplifier 261 and communicated to interface 22 through connection 268.

35 Recognition and comparison for the personal, biometric authentication system is based initially on fingerprint recognition followed by analysis of the biometric sensor signals for: EKG 126, NIR light at 910 nanometer 198-A and 198-C and at 660 nanometer 208-A and 208-C, and temperature 272. Authentication is processed in an embedded logic program within computer 6 using programming written in WATCOM C version 9.5 from WATCOM International Corp, Waterloo, Ontario, Canada computer code in a manner known to those skilled in the art. Description of the recognition subsystems, comparison subsystems, and authentication subsystems is shown in FIG 7. Alternatively, authentication can be processed using neural network programming in a manner known to those skilled in the art.

40 Authentication processing as shown in FIGURE 7 is started with keying in a PIN by the individual seeking personal authentication or by insertion of an ID card communicating a PIN identification 300. The individual places his or her hands in the locations shown in FIGS. 2a-2c and the individual's fingerprints are scanned 340 and processed to obtain the reference vector 342. The appropriate record 344 is recalled from memory 16 and compared 346 for acceptance or rejection. If the comparison is rejected, authentication has failed, regardless of the comparison arising from the non-specific biometric parameters. In a preferred embodiment, access is denied because of the rejected authentication.

45 In parallel with the recognition and comparison subsystems used for fingerprint recognition with data from finger-print storage, the non-specific biometric recognition steps are started concurrently as shown in FIG 7.

50 Biometric data are recognized and collected 310 over multiple samples (about 128) of the EKG signal, optical signals, and optional temperature signal taking a period of approximately 3.2 seconds with EKG signal preferably collected in a period of about 0.5 seconds. The logic process then proceeds to analyze the plethysmographic, EKG, and temperature signals by smoothing the optical and EKG signals using a five point rolling average 320, finding the major peaks in the EKG and 910 nm optical signals 322, calculating pulse rate of EKG and optical signals 324, finding valleys in the 910 nm NIR signal 326, calculating the oxygen saturation ratio from 660 nanometer and 910 nanometer optical signals 328, and averaging the temperature signal and calculating the average actual skin temperature 330.

55 Next a comparison 332 is made of the pulse rate obtained concurrently by the 910 nm optical plethysmography signal and the EKG signals. If the pulse rate as measured by both methods is within an acceptable synchronicity, then logic processing continues. If there is no acceptable synchronicity, then the authentication is rejected 352, regardless of the results of the comparison 346 of fingerprint identification.

EP 0 752 143 B1

If the two pulse rates are within acceptable synchronicity, then physiological norms of oxygen saturation, pulse, and temperature are recalled 334 for comparison 336 with the calculated oxygen saturation ratio 328, the pulse rate 324, and the temperature 310. If there is acceptable comparison 336, then with an acceptable fingerprint comparison 346, there is authentication 350. If there is no acceptable comparison 336, then authentication is rejected 354 regardless of the results of fingerprint comparison 346. As presently preferred, authentication subsystem then grants access to equipment or facilities.

FIG. 8 is the detail circuit diagram of the EKG circuit shown as a block diagram in FIG 4. TABLE 1. is the listing of components and devices used in this circuit.

10

TABLE 1

COMPONENTS	
B1,B2	NE2H Lamp
C1,C2	500pf
C3	200pf
C4,C5,C8	1μf
C6,C7	10μf
C9,C10,C11,C12,C13,C14	.056μf
R2,R1	300K
R3,R4,R7	50K
R5,R6	5M
R8,R9,R10,R11,R12	20K
R13,R34	2.2K
R14	30K
R16	1M
R17	4.75K
R18	47K
R19,R20,R21,R22,R23,R24	10K
R35	100
R36,R37	22K
R64	.1K
DEVICES	
U1,U3, U4	LF444CN
Operation Amplifier: National Semiconductor Santa Clara, CA	
U2	ISO107A
High Voltage Isolation Amplifier Burr-Brown Tucson, AZ	
D1,D2,D3,D4	1N4148
D6,D7	1N914
Diode: National Semiconductor Santa Clara, CA	

15

20

25

30

35

40

45

50

FIG. 9 is the detail circuit diagram of the blood oximeter light power circuit shown as a block diagram 140 in FIG 5. TABLE 2 is the listing of components and devices used in this circuit.

TABLE 2

COMPONENTS	
C21	1.0μf
C19	0.01μf
C20	4700pf

## EP 0 752 143 B1

TABLE 2 (continued)

COMPONENTS	
6	C22 C25 C32 C40 R40 R41 R46,R49,R50 R38 R39 R45,R43 R47,R48 R42,R44,R51
10	4.9 $\mu$ f 5.3 $\mu$ f 5.4 $\mu$ f 1 $\mu$ f 1M 47K 10K 1K 200K 4.7K 470 $\Omega$ 10 $\Omega$
15	
DEVICES	
20	U9 Clock/Timer: National Semiconductor Santa Clara, CA
25	U10 Analog Switch: Siliconix Santa Clara, CA
30	D5 Diode: National Semiconductor Santa Clara, CA
35	Q1,Q2 Q3,Q4,Q5,Q6 Transistor: National Semiconductor Santa Clara, CA
40	U4 Operational Amplifier National Semiconductor Santa Clara, CA
45	U14 Gate National Semiconductor Santa Clara, CA
	LM555CN - 1500 Hz DG211 1N4148 2N4403 2N4401 LF444C4 74HCT04

FIG. 10 is the detail circuit diagram of the blood oximeter read circuit shown as a block diagram 170 in FIG 5.  
 TABLE 3 is the listing of components and devices used in this circuit.

TABLE 3

COMPONENTS	
50	C42,C43 C44,C45,C47,C48,C49, C50,C52,C53,C56
55	C57 R15 R54,R55,R56,R57, R62,R63,R64,R65
	0.1 $\mu$ f 0.47 $\mu$ f 10pf 10M 25K 560 1.0M
	R52,R53 R66,R58

TABLE 3 (continued)

COMPONENTS	
R67,R59	5K
R60,R68	330K
DEVICES	
U6, U7, U8 Operation Amplifier:  National Semiconductor, Santa Clara, CA	LF444CN
U12,U11 Sample and Hold: National Semiconductor, Santa Clara, CA	LF398

FIG. 11 is the detail circuit diagram of the temperature sensor circuit shown as block diagrams 250 and 260 in FIG 6. TABLE 4 is the listing of components and devices used in this circuit.

TABLE 4

COMPONENTS	
C15	1.0μf
R30	475K
R26,R29,R32,R33	4.75K
R28,R25	100K
R27	23.5K
R31	240K
DEVICES	
U4 Operation Amplifier: National Semiconductor Santa Clara, CA	LF444CN
DS1 Murata Manufacturing Co. Ltd. Kyoto, Japan	E10051
T2 National Semiconductor Santa Clara, CA	LM34

While embodiments of the invention have been disclosed, the following claims disclose the scope of the invention.

#### Claims

1. A biometric, personal authentication system, comprising:

- (a) storage subsystem to store a unique, inherently specific biometric parameter from at least one individual in a species;
- (b) first detection subsystem to detect the unique, inherently specific biometric parameter in an individual seeking personal authentication;
- (c) second detection subsystem to detect at least one non-specific biometric parameter of a physiological characteristic having measurable variability during the time of authentication in the individual seeking personal authentication;
- (d) first comparison subsystem to compare the unique, inherently specific biometric parameter detected by

- the first detection subsystem with the unique, inherently specific biometric parameter stored in the storage subsystem;
- (e) second comparison subsystem to compare each non-specific biometric parameter to physiological norms for the species; and
- 6 (f) authentication subsystem to confirm identity of the individual seeking personal authentication by evaluating the comparisons made by first comparison subsystem and second comparison subsystem.
2. The system according to Claim 1, wherein second detection subsystem detects and second comparison subsystem compares at least two non-specific biometric parameters with a physiological correlation between the two non-specific biometric parameters within an acceptable range.
- 10 3. The system according to Claims 1-2, wherein storage subsystem is used to limit database searching by processing a personal identification code number; or wherein storage subsystem is resident on a card possessed by an individual or wherein the storage subsystem also enrolls data of the unique, inherently biometric detection system.
- 15 4. The system according to Claims 1-3, wherein the non-specific biometric parameter is selected from the group consisting of pulse rate, electrocardiographic signals, spectral characteristics of human tissue, percentage oxygenation of blood, bloodflow, hematocrit, biochemical assays of tissue, electrical plethysmography, skin exudates, mechanical properties of skin, transportation of gases, blood pressure, differential blood volumes, and combinations thereof.
- 20 5. The system according to Claims 1-4, wherein the non-specific biometric parameters further include skin temperature.
- 25 6. The system according to Claims 1-5, wherein the unique, inherently specific biometric parameter is selected from the group consisting of fingerprint, pore print, palm print, voice print, and retinal configuration.
7. The system according to Claims 1-6, further comprising an access subsystem to measure alcohol or controlled chemical substance levels in blood of an individual successfully authenticated.
- 30 8. Equipment comprising the system of Claims 1-7 to control access to a facility by authentication of an individual using the system of Claims 1-7.
9. The equipment according to Claim 8 wherein the system further comprises an access subsystem to measure alcohol or controlled chemical substance levels in blood of an individual successfully authenticated and wherein access to the equipment is controlled by the access subsystem after an individual is successfully authenticated.
- 35 10. A method to authenticate an individual using the system of Claims 1-7 comprising the steps of:
- 40 (a) placing both hands of an individual in a device containing the system of Claims 1-7 that concurrently recognizes a unique, inherently specific biometric parameter and recognizes at least one non-specific biometric parameter of a physiological characteristic having measurable variability during the time of authentication; and
- (b) comparing biometric parameters detected by the system of Claims 1-7 to confirm identity of the individual seeking personal authentication.

**Patentansprüche**

1. Biometrisches Personenaufentifizierungssystem mit:
- 50 (a) einem Speicherteilsystem zum Speichern eines einmaligen, inhärent spezifischen biometrischen Parameters mindestens eines Individuums einer Art;
- (b) einem ersten Nachweisteilsystem zum Nachweis des einmaligen, inhärent spezifischen biometrischen Parameters eines um persönliche Authentifizierung ersuchenden Individuums;
- 55 (c) einem zweiten Nachweisteilsystem zum Nachweis mindestens eines nichtspezifischen biometrischen Parameters eines physiologischen Merkmals des um persönliche Authentifizierung ersuchenden Individuums; das während der Zeitdauer der Authentifizierung meßbar veränderlich ist;
- (d) einem ersten Vergleichsteilsystem zum Vergleichen des durch das erste Nachweisteilsystem nachgewie-

EP 0 752 143 B1

sönen einmaligen, inhärent spezifischen biometrischen Parametern mit dem im Speicherteilsystem gespeicherten einmaligen, inhärent spezifischen biometrischen Parameter;  
5 (e) einem zweiten Vergleichsteilsystem zum Vergleichen jedes nichtspezifischen biometrischen Parameters mit physiologischen Normdaten für die Art; und  
(f) einem Authentifizierungsteilsystem zum Bestätigen der Identität des um persönliche Authentifizierung ersuchenden Individuums durch Auswerten der durch das erste und das zweite Vergleichsteilsystem erhaltenen Vergleichsergebnisse.

- 10 2. System nach Anspruch 1, wobei mindestens zwei nichtspezifische biometrische Parameter durch das zweite Nachweisteilsystem nachgewiesen und durch das zweite Vergleichsteilsystem verglichen werden, wobei innerhalb eines Toleranzbereichs eine physiologische Korrelation zwischen den beiden nichtspezifischen biometrischen Parametern besteht.
- 15 3. System nach Anspruch 1 oder 2, wobei das Speicherteilsystem verwendet wird, um die Datenbanksuche zu begrenzen, indem eine Personenidentifizierungs-Codenummer verarbeitet wird, oder wobei das Speicherteilsystem auf einer im Besitz eines Individuums befindlichen Karte vorhanden ist oder wobei das Speicherteilsystem auch Daten des einmaligen, inhärent biometrischen Erfassungssystems enthält.
- 20 4. System nach einem der Ansprüche 1 bis 3, wobei der nichtspezifische biometrische Parameter aus der Pulsfrequenz, elektrokardiographischen Signalen, Spektralmerkmalen des menschlichen Gewebes, der prozentualen Sauerstoffaufnahme des Blutes, der Perfusion, dem Hämatokrit, biochemischen Gewebeuntersuchungen, der elektrischen Plethysmographie, Hautexsudaten, mechanischen Eigenschaften der Haut, Gastransporteigenschaften, dem Blutdruck, differentiellen Blutvolumina und Kombinationen davon ausgewählt wird.
- 25 5. System nach einem der Ansprüche 1 bis 4, wobei die nichtspezifischen biometrischen Parameter außerdem die Hauttemperatur umfassen.
- 30 6. System nach einem der Ansprüche 1 bis 5, wobei der einmalige, inhärent spezifische biometrische Parameter aus einem Fingerabdruck, Porenabdruck, Handflächenabdruck, Stimmabdruck und der Netzhautstruktur ausgewählt wird.
- 35 7. System nach einem der Ansprüche 1 bis 6, das ferner ein Zutritts- oder Zugriffsteilsystem zum Messen des Alkoholgehalts oder des Gehalts einer kontrollierten chemischen Substanz im Blut eines erfolgreich authentifizierten Individuums aufweist.
- 40 8. Vorrichtung mit dem System nach einem der Ansprüche 1 bis 7 zur Steuerung des Zutritts oder Zugriffs zu einer Einrichtung durch Authentifizieren eines Individuums unter Verwendung des Systems nach einem der Ansprüche 1 bis 7.
9. Vorrichtung nach Anspruch 8, wobei das System außerdem ein Zutritts- oder Zugriffsteilsystem zum Messen des Alkoholgehalts oder des Gehalts einer kontrollierten chemischen Substanz im Blut eines erfolgreich authentifizierten Individuums aufweist und wobei der Zutritt oder Zugriff zu der Einrichtung durch das Zutritts- oder Zugriffsteilsystem gesteuert wird, nachdem ein Individuum erfolgreich authentifiziert ist.
- 45 10. Verfahren zum Authentifizieren eines Individuums unter Verwendung des Systems nach einem der Ansprüche 1 bis 7, mit den Schritten:  
50 (a) Anordnen beider Hände eines Individuums in einer vorrichtung, die das System nach einem der Ansprüche 1 bis 7 aufweist, das einen einmaligen, inhärent spezifischen biometrischen Parameter und gleichzeitig mindestens einen nichtspezifischen biometrischen Parameter eines physiologischen Merkmals erkennt, das während der Zeitdauer der Authentifizierung messbar veränderlich ist; und  
(b) Vergleichen der durch das System nach einem der Ansprüche 1 bis 7 nachgewiesenen biometrischen Parameter, um die Identität des um persönliche Authentifizierung ersuchenden Individuums zu bestätigen.

55 **Revendications**

1. Un système d'authentification personnelle biométrique comprenant:

- (a) un sous-système de mémorisation pour mémoriser un paramètre biométrique spécial, spécifique de façon inhérente, provenant d'au moins un individu d'une espèce;
- 5 (b) un premier sous-système de détection pour détecter dans un individu qui recherche une authentification personnelle le paramètre biométrique spécial, spécifique de manière inhérente;
- (c) un deuxième sous-système de détection pour détecter au moins un paramètre biométrique non spécifique d'une caractéristique physiologique à variabilité mesurable, dans l'individu recherchant une authentification personnelle, pendant le temps d'authentification;
- 10 (d) un premier sous-système de comparaison pour comparer le paramètre biométrique spécial, spécifique de façon inhérente, détecté par le premier sous-système de détection au paramètre biométrique spécial, spécifique de manière inhérente, mémorisé dans le sous-système de mémorisation;
- 15 (e) un deuxième sous-système de comparaison pour comparer à des normes physiologiques de l'espèce chaque paramètre biométrique non spécifique; et
- (f) un sous-système d'authentification pour confirmer l'identité de l'individu qui recherche une authentification personnelle en évaluant les comparaisons effectuées par le premier sous-système de comparaison et le deuxième sous-système de comparaison.
- 20
2. Le système selon la revendication 1 dans lequel le deuxième sous-système de détection détecte et le deuxième sous-système de comparaison compare au moins deux paramètres biométriques non spécifiques, une corrélation physiologique entre les deux paramètres biométriques non spécifiques étant comprise à l'intérieur d'une plage acceptable.
- 25
3. Le système selon l'une des revendications 1 ou 2, dans lequel le sous-système de mémorisation est utilisé pour limiter une recherche en base de données en traitant un numéro de code d'identification personnel; ou dans lequel le sous-système de mémorisation est résidant sur une carte possédée par un individu ou dans lequel le sous-système de mémorisation inscrit aussi des données du système de détection spécial biométrique de façon inhérente.
- 30
4. Le système selon l'une des revendications 1 à 3, dans lequel le paramètre biométrique non spécifique est sélectionné dans le groupe constitué par le pouls, des signaux électrocardiographiques, des caractéristiques spectrales d'un tissu humain, un pourcentage d'oxygénation du sang, l'écoulement sanguin, un hématocrite, des dosages biochimiques d'un tissu, une pléthysmographie électrique, des exsudats de la peau, des propriétés mécaniques de la peau, un transport de gaz, une pression sanguine, des volumes sanguins différentiels, et des combinaisons de ceux-ci.
- 35
- 40 5. Le système selon l'une des revendications 1 à 4, dans lequel les paramètres biométriques non spécifiques incluent en outre la température de la peau.
6. Le système selon l'une des revendications 1 à 5, dans lequel le paramètre biométrique spécial, spécifique de façon inhérente est sélectionné à partir du groupe constitué par des empreintes digitales, des empreintes de pores, des empreintes de paumes, une empreinte vocale et une configuration rétinienne.
- 45
7. Le système selon l'une des revendications 1 à 6 qui comprend en outre un sous-système d'accès pour mesurer, dans le sang d'un individu authentifié avec succès, des niveaux d'alcool ou d'une substance chimique contrôlée.
- 50 8. Equipment comprenant le système selon l'une des revendications 1 à 7, pour commander l'accès à une installation par authentification d'un individu en utilisant le système selon l'une des revendications 1 à 7.
9. L'équipement selon la revendication 8 dans lequel le système comprend en outre un sous-système d'accès pour mesurer, dans le sang d'un individu authentifié avec succès, des niveaux d'alcool ou d'une substance chimique contrôlée et dans lequel l'accès à l'équipement est commandé par le sous-système d'accès après authentification réussie d'un individu.
- 55
10. Un procédé d'authentification d'un individu en utilisant le système selon l'une des revendications 1 à 7 comprenant

EP 0 752 143 B1

les étapes consistant à:

- (a) placer les deux mains d'un individu dans un dispositif contenant le système selon l'une des revendications 1 à 7 qui, simultanément, reconnaît un paramètre biométrique spécial, spécifique de façon inhérente, et reconnaît au moins un paramètre biométrique non spécifique d'une caractéristique physiologique à variabilité mesurable pendant la période d'authentification; et

(b) comparer des paramètres biométriques détectés par le système selon l'une des revendications 1 à 7 afin de confirmer l'identité de l'individu qui recherche une authentification personnelle.

10

15

20

25

30

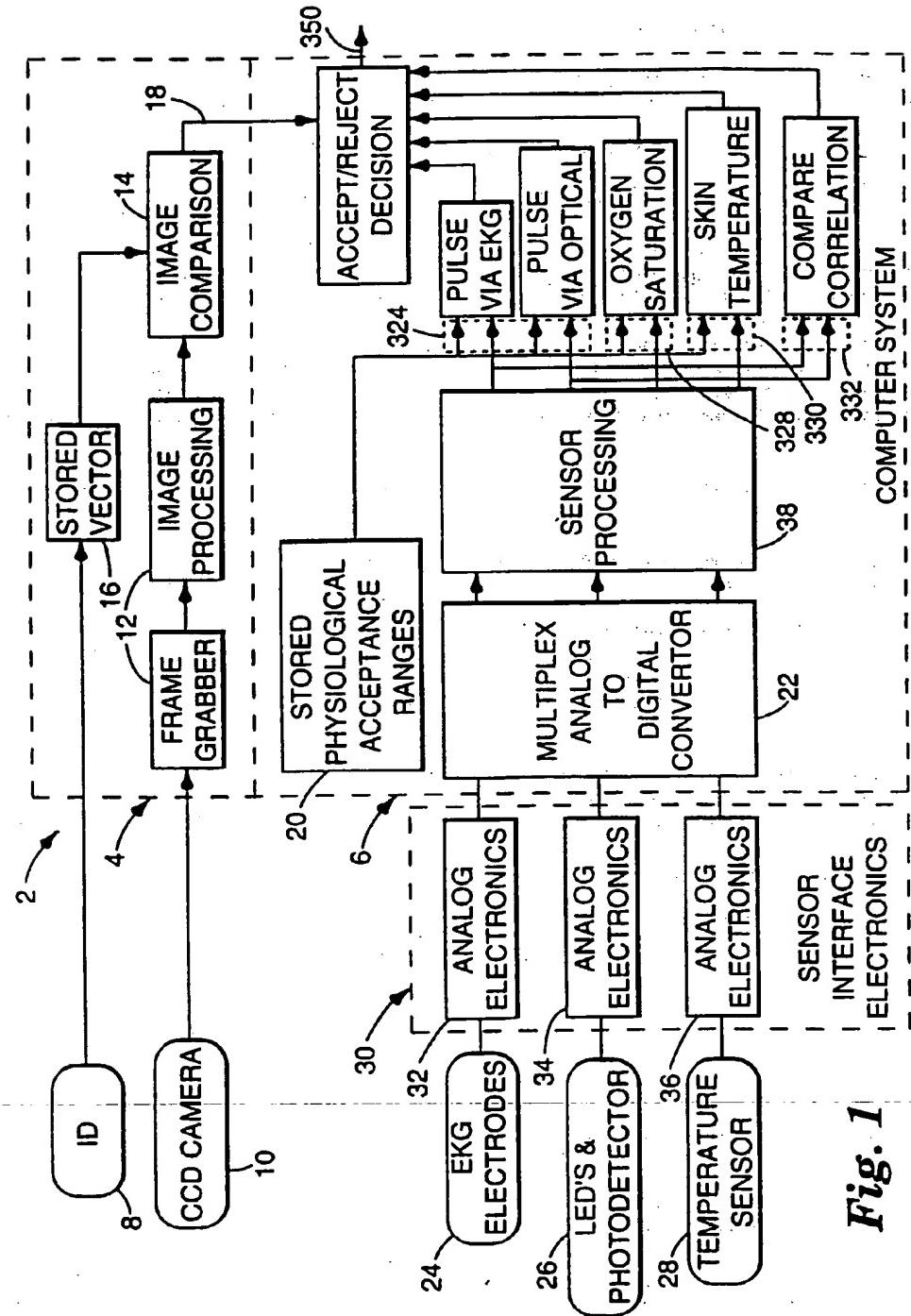
1

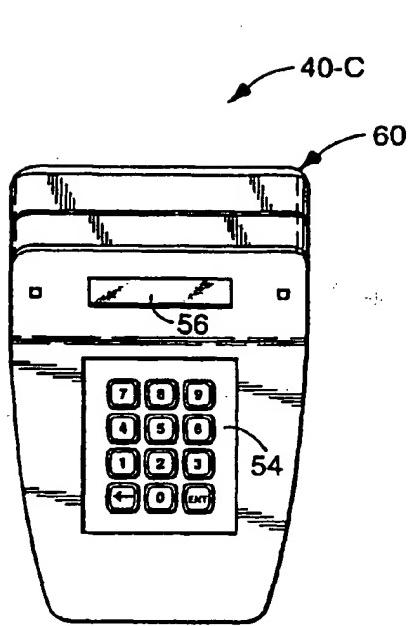
40

45

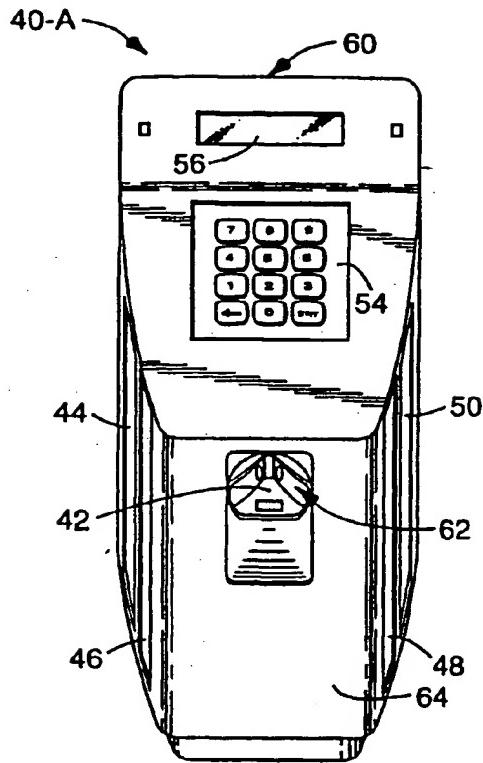
50

55

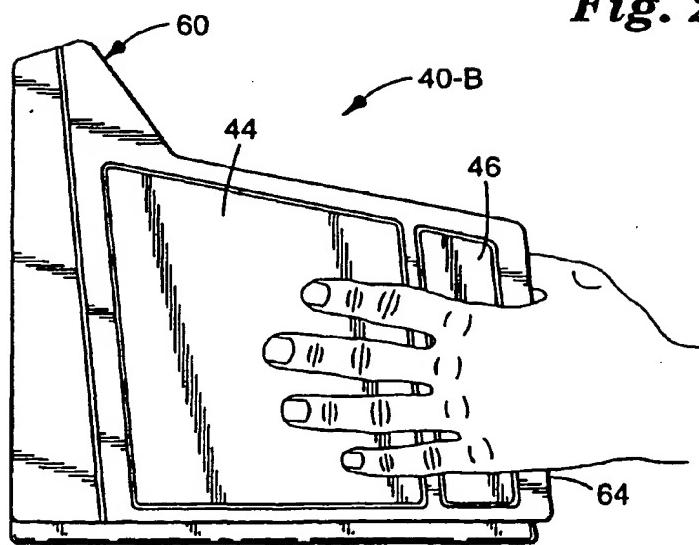
**Fig. 1**



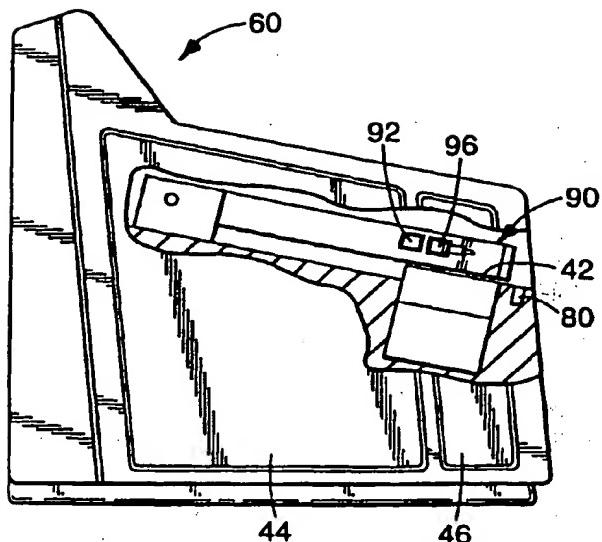
*Fig. 2c*



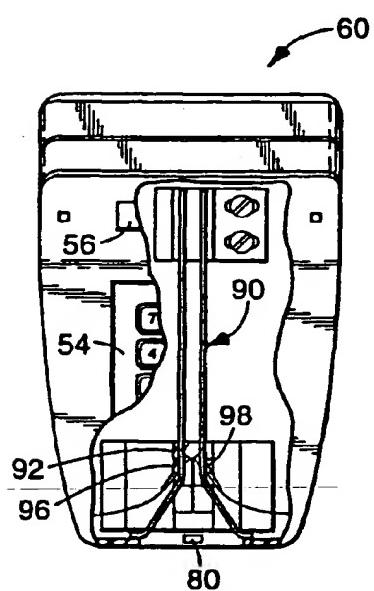
*Fig. 2a*



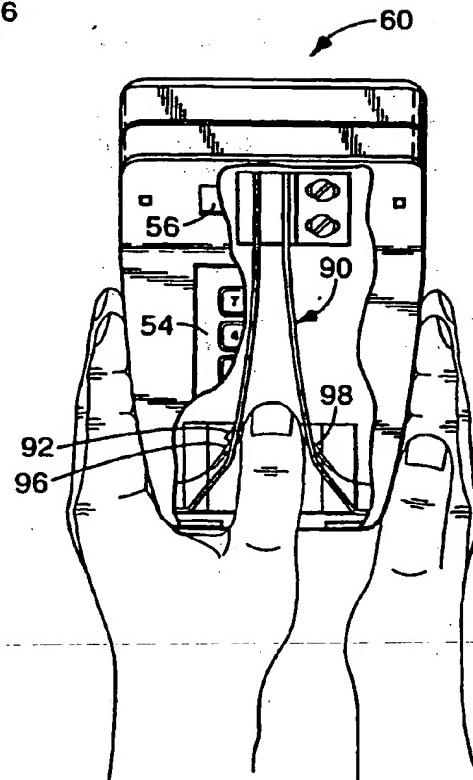
*Fig. 2b*



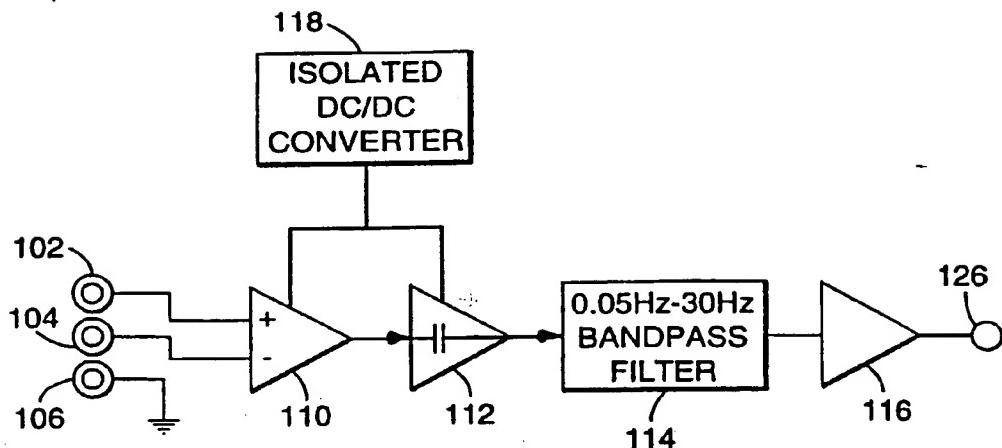
*Fig. 3a*



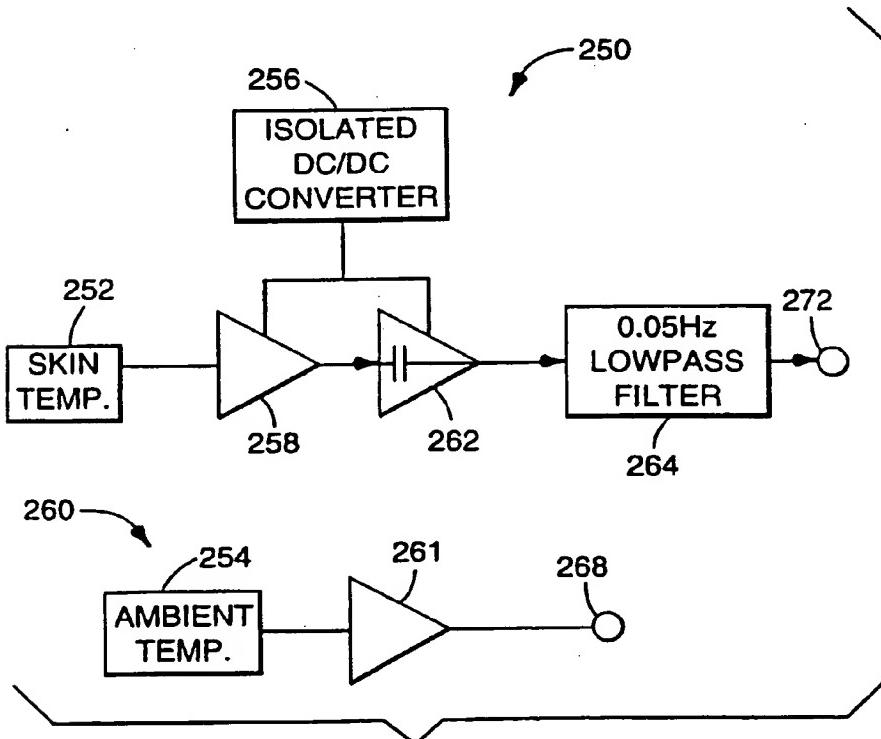
*Fig. 3b*



*Fig. 3c*

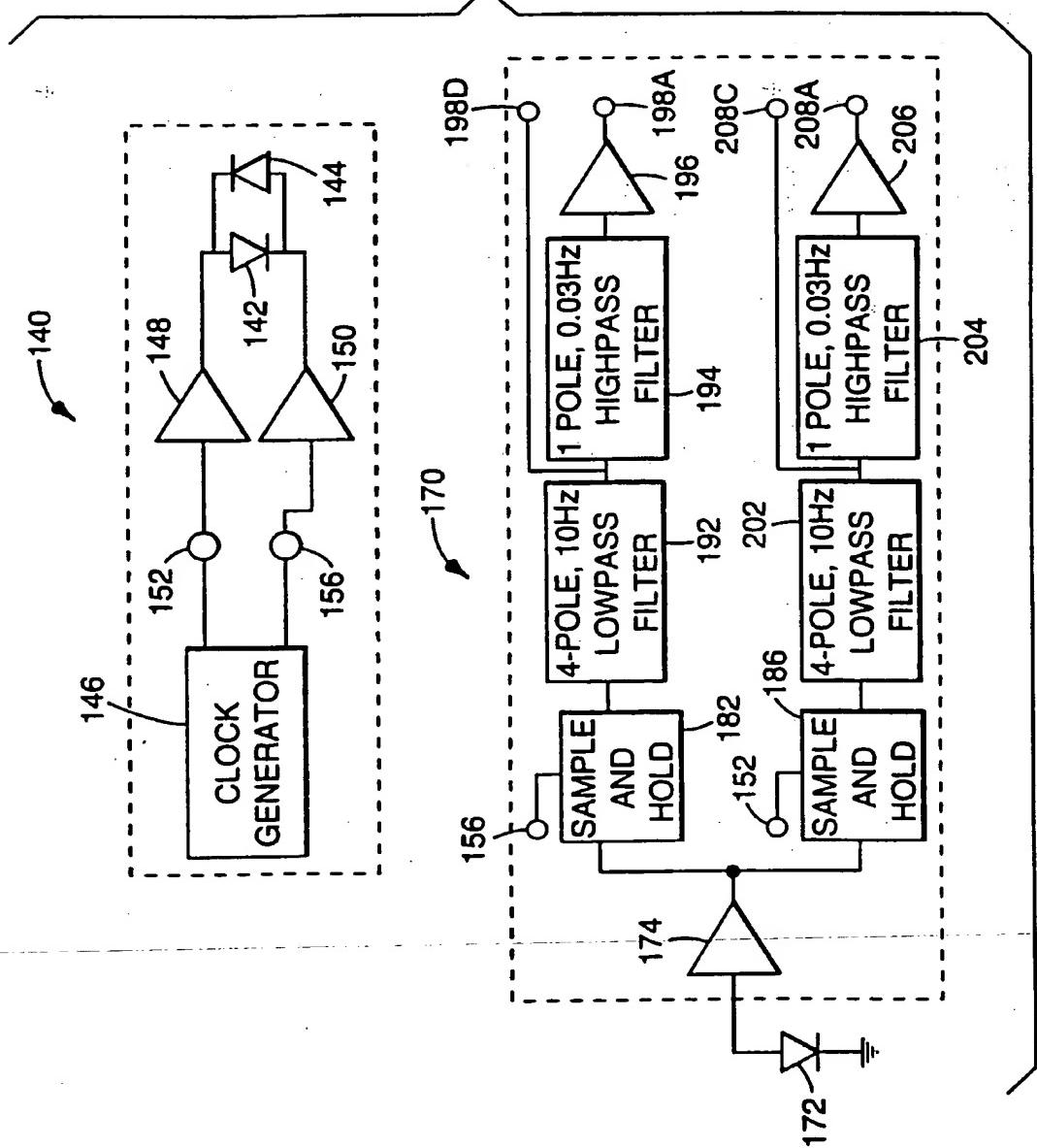


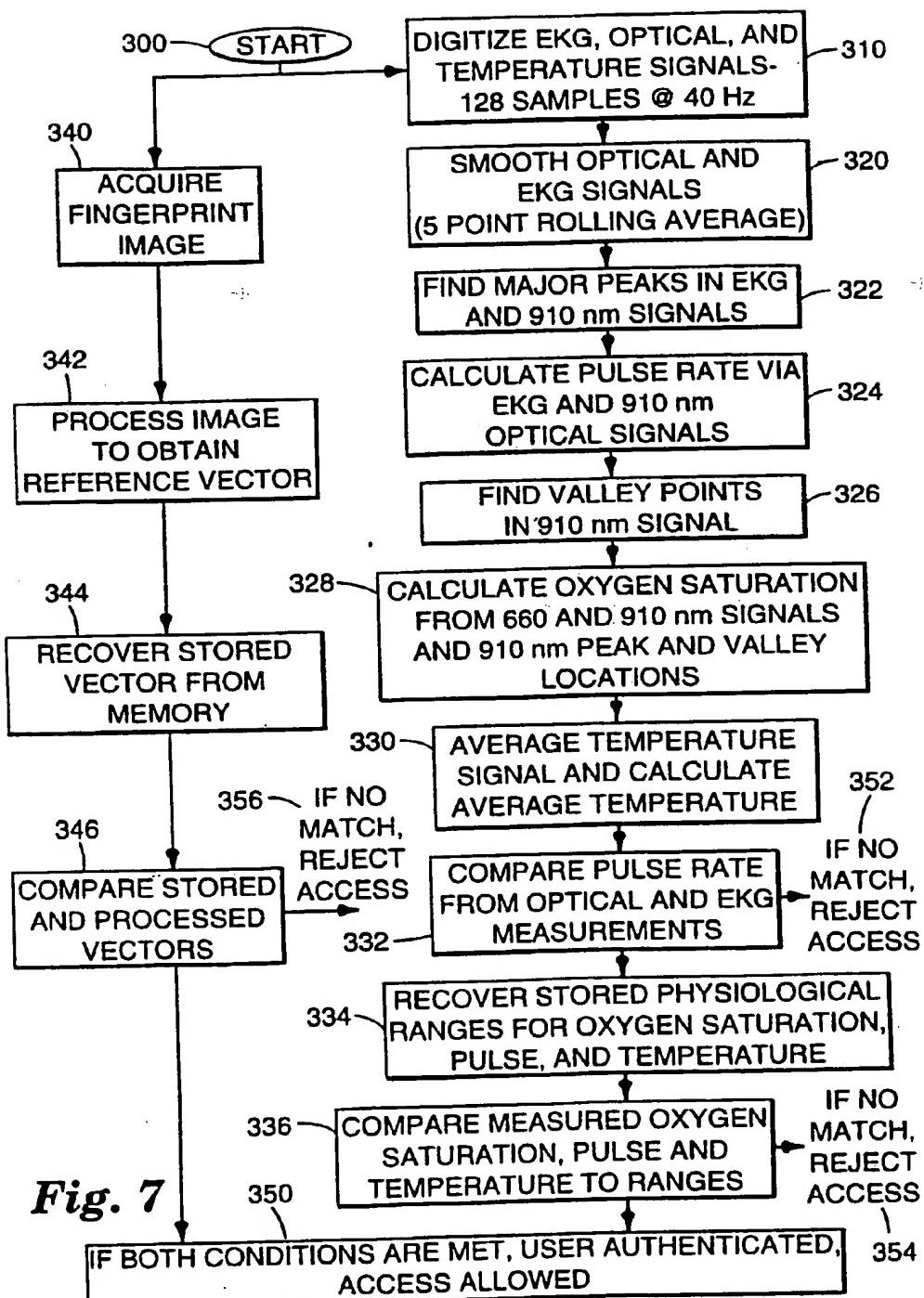
*Fig. 4*



*Fig. 6*

Fig. 5





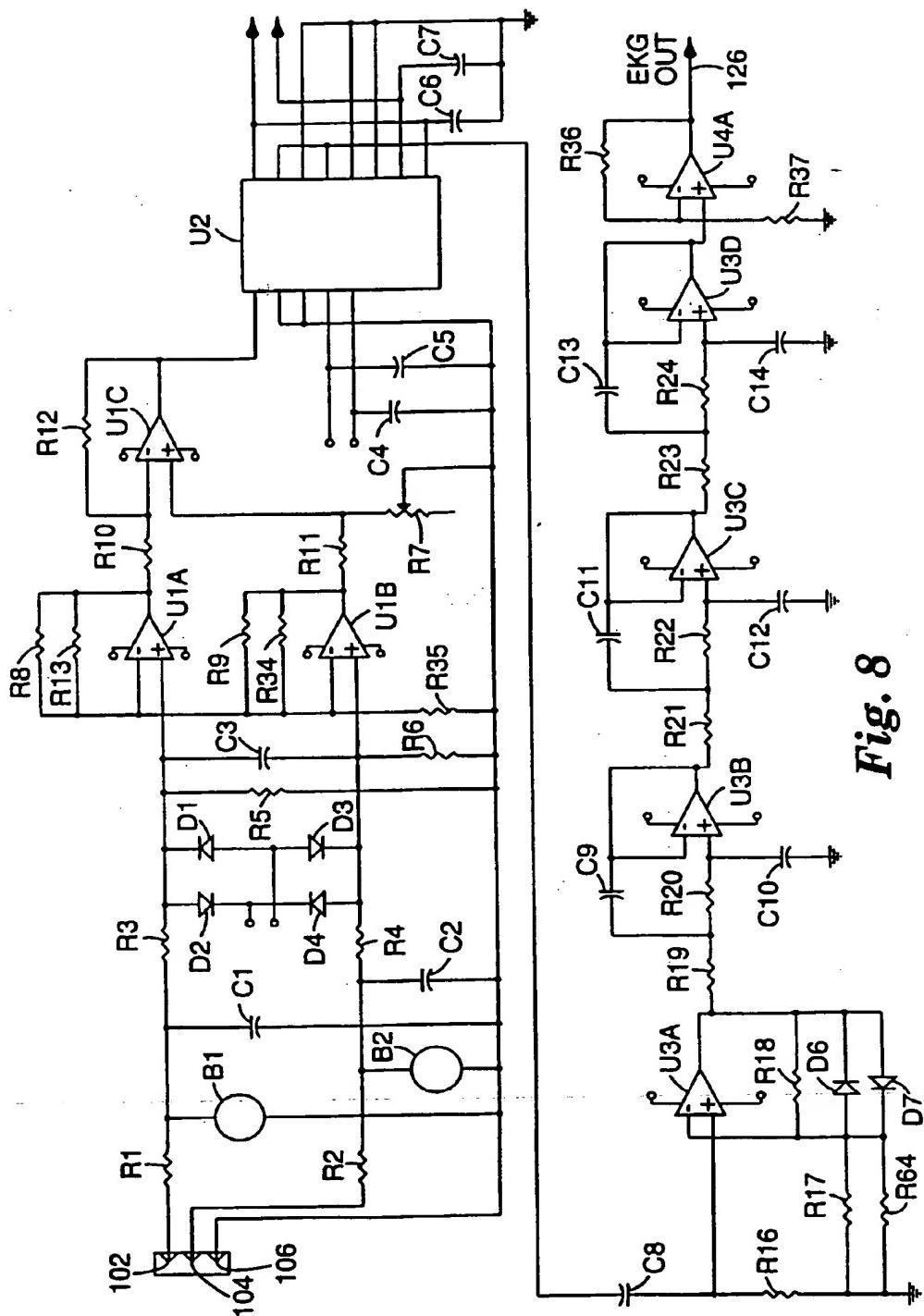


Fig. 8

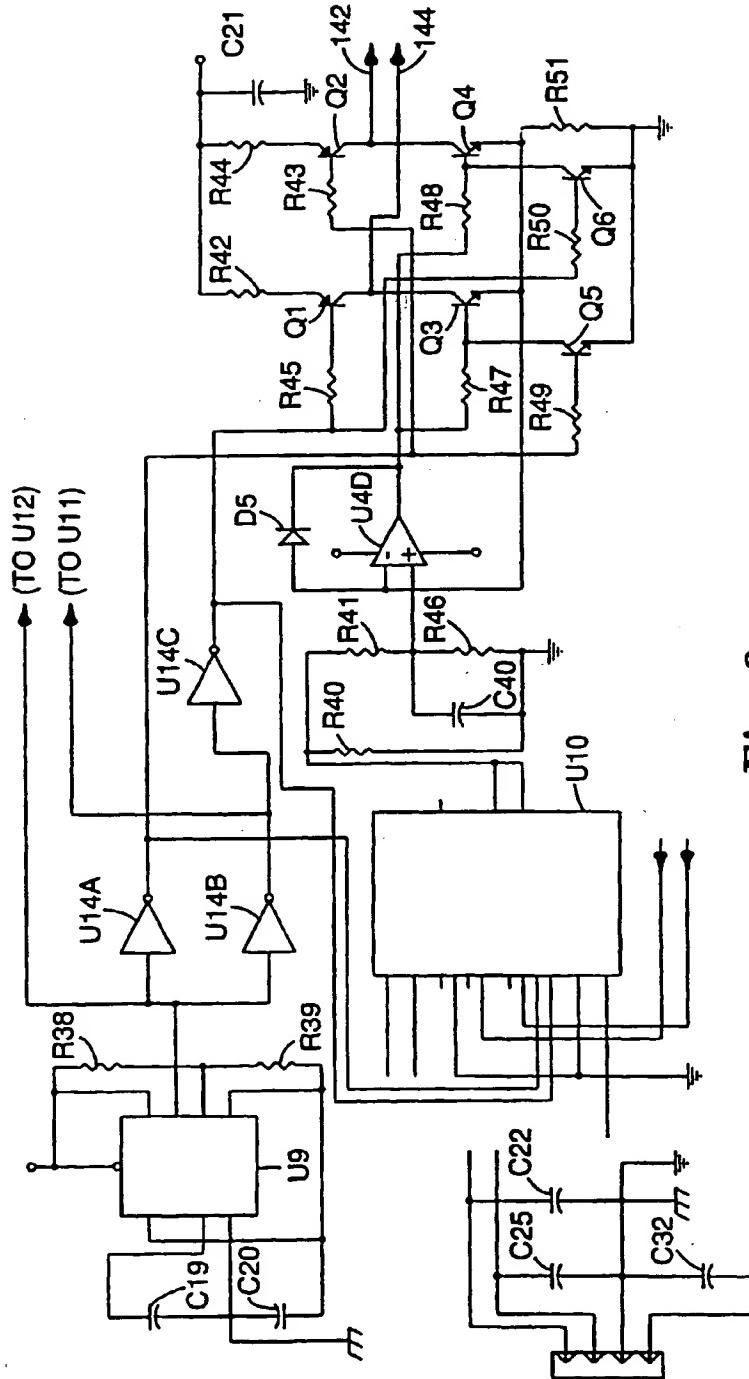


Fig. 9

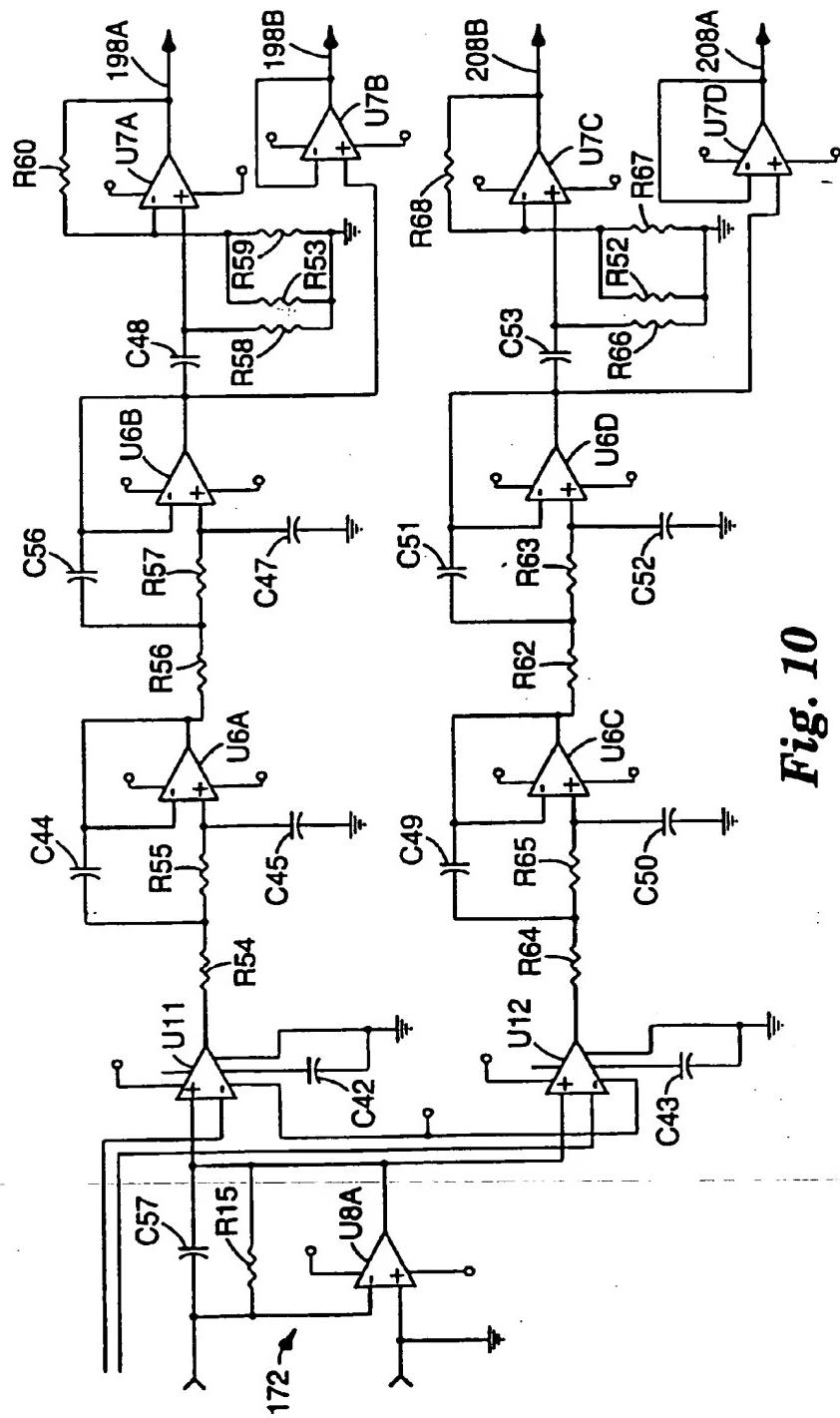


Fig. 10

